LAPTOP SECURITY

In this tutorial, you will learn:

- The basics of laptop security
- Common laptop security vulnerabilities
- How to prevent laptop theft
- How to prevent laptop damage
- How to keep your computer safe from malicious code
- How to prevent unauthorized access to secure information contained in your laptop

An Introduction to Laptop Security

Because of their portability, laptops are often used in non-secure areas and can readily come into contact with hazardous situations that can compromise data.

YOUR ARE THE FIRST LINE OF DEFENSE

Your laptop can be easily stolen, damaged, infected by malicious code, and accessed by unauthorized users. Only by understanding the threats can you keep your laptop safe.

COMMON LAPTOP VULNERABILITIES

There are security risks to the confidentiality, integrity, and availability of data in your work environment.

Since you are responsible for your computer workstation's security, you should understand these vulnerabilities and make sure protective measures are in place.

Theft, damage, malicious code, residual data, electronic emanations, unauthorized access … these are some of the common ways that information on a workstation computer can be jeopardized.

The 4 Most Common Threats to Your Laptop's Security

1. **THEFT**
2. **DAMAGE**
3. **MALICIOUS CODE**
4. **UNAUTHORIZED ACCESS**

1. THEFT

There have been at least three separate incidents of theft to Navy Recruiting Stations and vehicles within the past 2 years. At least 6 Recruiter's laptops were stolen.

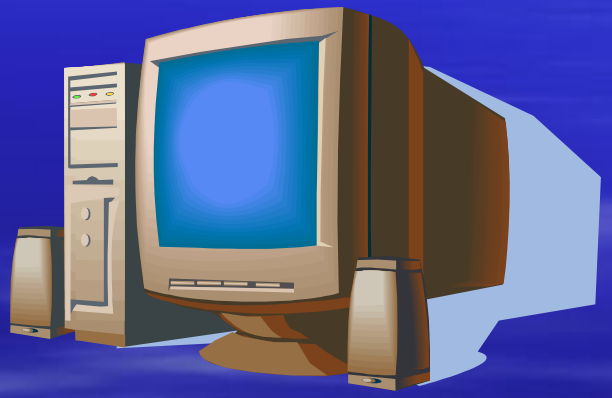
Like all valuable office equipment, your government issued personal computers, particularly laptops, are targets for theft. Your computers have additional value, far exceeding the cost of the hardware itself, because they store sensitive data.

Your computer equipment must be protected from theft so that DoD data does not fall into the wrong hands.

What Was Lost?

If your computer is stolen, what type of information is contained i

- Names
- Birthdates
- Social Security Numbers
- Family Information
- Places of Birth
- Citizenship Status
- Drug Usage History
- Medical History



Can you think of anything else? What would happen if this information got into the wrong hands?

The Real Value of Your Computer

Your computer and all it's peripherals are valued at $3,810.96. If it were stolen, your computer alone could be sold for around $300. But, what is the information contained in your computer really worth?

The average Rinc has about 4,000 applicants on his/her Rtools Database with several more names added on a daily basis. This is an identity thief's dream come true considering that the average cost of a stolen identity is about $6,000.

THAT'S POTENTIALLY $24,000,000!!

What About Your Credibility?

As Navy recruiters, you're already perceived in the same category as used car salesmen. Your integrity is in question on a daily basis. Now add to that the stigma of having lost 4000 names, SSN's, birthdates, etc.

Applicants trust you with their personal information. Information they wouldn't normally reveal to anyone. Plus, you tell them that everything they say is covered by the Privacy Act, and that it'll stay between you, them, and the U.S. Navy.

No one mentioned anything about their information being available to identity thieves!

What steps do you need to take to ensure the information contained in your computer remains safe?

Preventing Theft

Theft of your government issued computer equipment can be prevented by following some simple steps.

- Keep equipment safe from theft with physical security and inventory controls. You are the physical security at your NRS. Keep positive control of your assets.

- Use physical security measures such as enclosures and lockdown devices (i.e. safes, locked cabinets).

2. DAMAGE

There are two main types of damage that you need to protect your computer against:

- Physical Damage
- Electronic Damage

Protecting Your Laptop from Physical Damage

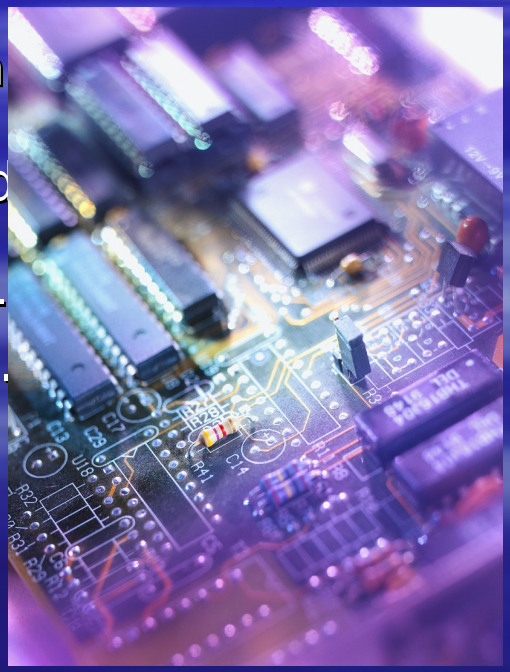
Your government issued laptop is made up of electronic circuits protected by plastic. It is susceptible to damage if not treated properly. Protecting it from physical damage can be as simple as using some common sense. Here are some helpful tips:

- Treat it as if it is your own.
- When on the road, use your computer case to protect it.
- Shut off your computer when not in use.
- Limit access to authorized users only.
- Do not eat or drink near your computer.
- Keep your computer in a safe place when you secure for the day.
- Can you think of anything else?

Protecting Your Laptop from Electronic Damage

Physical damage is not the only type you have to worry about. It's also possible to damage not only the circuitry of your laptop, but also its installed programs and operating system to the point where your laptop becomes inoperable. Here are some helpful tips to help you avoid electronic damage.

- Do not download or install non-approved progra software, or applications.
- Keep your computer's antivirus program up-to-d and run periodic scans.
- Keep your operating system patched and up-to-
- Use care when opening email with attachments.
- Limit access to authorized users only.
- Do not eat or drink near your computer.
- Can you think of anything else?



What to do in Case Your Computer is Damaged

In case your computer is physically (dropped, keys broken or missing, screen cracked, liquid spill, etc.), or electronically (Virus attack, Trojan horse, worm, spyware, etc.) damaged, the first thing you should do is contact your Sysad department. We will be able to help you.

WORD OF CAUTION: We can replace broken equipment, we can get rid of malware, but we may not be able to replace lost data. It's important that you back up all important information regularly.

Most of you already back up your Rtools on a regular basis, and that's part of your job. But, think about this for a second: What would the consequences be if your computer was totally damaged and you lost all your data? How many of you back up other important files? That means all your emails, applicant kits, PEWs, or whatever else is important to you.

Having a back-up system for your computer will keep a safe copy of all your data, which can then be reloaded onto your new or repaired computer if and when the unthinkable happens.

3. MALICIOUIS CODE

Often called Malware, malicious code can include viruses, worms, Trojan horses, and other types of code that can damage applications, operating systems, and data.

You should understand how these programs work and make sure your computer systems are protected.

Understanding Malware

Malware is a general term used to describe software used to infiltrate and/or damage your computer system. These can include:

- Spyware
- Adware
- Worms
- Trojan Horses
- Viruses

Spyware

Spyware is computer software that collects personal information about you without your informed consent. The term is often used interchangeably with adware.

Spyware works by secretly recording your personal information by employing a variety of techniques. These include logging keystrokes, recording Internet web browsing history, and scanning documents on the computer's hard disk.

Adware

Adware or

supported

any

software package

which

automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used, often

Worms

A **worm** is a piece of software that uses computer networks and security flaws to create copies of itself. A copy of the worm will scan the network for any other machine that has a specific security flaw. It replicates itself to the new machine using the security flaw, and then begins scanning and replicating anew.

Worms will replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file.

Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm.

Trojan Horses

Trojan horses are impostor files that claim to be something desirable but, in fact, are malicious. Rather than insert code into existing files, a Trojan horse appears to do one thing (install a screen saver, or show a picture inside an e-mail for example) when in fact it does something entirely different, and potentially malicious, such as erase files.

Trojans can also open back doors so that computer hackers can gain access to passwords, and other personal information stored on a computer.

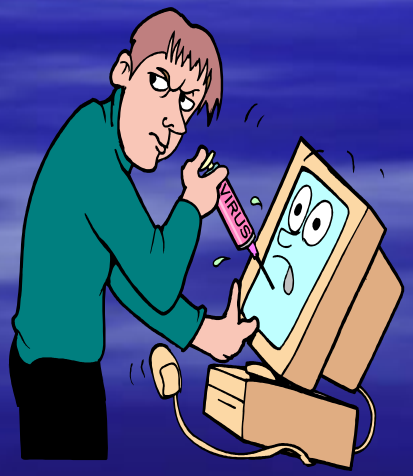
Although often referred to as such, Trojan horses are not viruses in the strict sense because they cannot replicate automatically. For a Trojan horse to spread, it must be invited onto a computer by the user opening an email attachment or downloading and running a file from the Internet.

Computer Viruses

A **computer virus** is a self-replicating computer program written to alter the way a computer operates, without the permission or knowledge of the user.

Though the term is commonly used to refer to a range of malware, a true virus must replicate itself, and must execute itself.

The latter criteria are often met by a virus which replaces existing executable files with a virus-infected copy. While viruses can be intentionally destructive —destroying data, for example— some viruses are benign or merely annoying.



Keeping Your Computer Free From Malware

It *is* possible to keep your computers healthy and free from malicious code. One way to do so is by restricting their use to DoD authorized activities.

For Official Use Only!!

As Navy Officers, Chief Petty Officers, and Petty Officers, you should know and understand what you are, and are not, allowed to do on your work computers.

Other Ways to Protect Your Computer from Malware

1. Your government issued computer already has an antivirus program. The virus definitions should be updated regularly, and a security scan should be run at least once per week.

2. Do not open email attachments from anyone you don’t know or recognize.

3. Keep your Microsoft Windows up-to-date by running updates, or by setting the computer to automatically download and install updates.

4. Do not download, and/or install software or programs not authorized by CNRC/NRD San Francisco.

4. UNAUTHORIZED ACCESS

Although new operating systems provide more and more security features to prevent unauthorized access, these features are simply not sufficient to protect sensitive DoD information.

How can you reduce the risk of unauthorized access?

Limit Physical Access

- Only authorized personnel should be allowed access to government issued computers.
- Store sensitive files on a server or removable disk instead of on your workstation's local hard drive
- Maintain positive control of all DoD computer assets.

Limiting Electronic Access

Preventing unauthorized access of your DoD laptop is not just about keeping it within arms reach at all times. You must also protect it from malicious code.

As outlined in a previous section, malicious code can range from benign yet annoying, to posing a serious security threat. It can allow hackers access to sensitive information, and give them the ability to not only view secure data, but also delete and destroy files and severely corrupt your operating system. Here are a few simple steps to prevent unauthorized electronic access to your laptop:

- Protect your computer by keeping antivirus programs and operating systems up-to-date
- Allow your antivirus program to run on a continuous basis.
- Refrain from downloading or installing unauthorized programs and software.
- Do not open email attachments from unknown sources.
- Use your computer for official purposes only in the conduct of your duties.

CONCLUSION

1. You are the first line of defense.
2. Prevent theft by maintaining positive control.
3. Prevent physical/electronic damage by treating your computer as your own.
4. Keep your computer healthy and malware-free by limiting its use for official use only, & keeping it up-to-date.
5. Prevent unauthorized access by insuring only you (and other authorized personnel) have physical access to it, and by following the steps above.